Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter	)	
	)	
Communications Assistance for Law Enforcement Act and Broadband Access And Services	)))	ET Docket No. 04-295 RM-10865

COMMENTS OF SBC COMMUNICATIONS

Jennifer Brown
Gary Phillips
Paul K. Mancini

SBC Communications Inc.
1401 Eye Street, NW
Suite 1100
Washington, D.C. 20005
(202) 326-8904 – phone
(202) 408-8745 – facsimile

Its Attorneys

November 8, 2004

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter	)	
	)	
Communications Assistance for Law	)	ET Docket No. 04-295
Enforcement Act and Broadband Access	)	
And Services	)	RM-10865

COMMENTS OF SBC COMMUNICATIONS INC.

SBC Communications Inc. (SBC) submits the following comments in response to the Commission's Notice of Proposed Rulemaking on the applicability of the Communications Assistance for Law Enforcement Act (*CALEA NPRM*) to broadband services and voice over Internet Protocol (VoIP) services.[1]

I. INTRODUCTION AND SUMMARY

SBC strongly supports Law Enforcement's[2] ability to conduct lawful surveillance activities and has been extremely cooperative in working with Law Enforcement to ensure its legitimate surveillance needs are met. SBC intends to continue this endeavor of cooperative assistance regardless of whether the Commission ultimately determines that broadband and VoIP services are subject to CALEA. Before making a determination that would extend CALEA requirements to broadband and VoIP services, the Commission should first understand the purpose of CALEA and the fact that Law Enforcement neither derives its ability to perform surveillance activities nor its ability to compel provider cooperation in those activities from

---

[1] *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, RM-10865, Notice of Proposed Rulemaking and Declaratory Ruling, 19 FCC Rcd 15676 (2004).

[2] Except as otherwise indicated in the text, the term Law Enforcement refers to all law enforcement agencies generally, including the FBI and DOJ as well as state and local law enforcement.

CALEA. Given that reality, the Commission should tread carefully in imposing additional, potentially unnecessary, regulations on these growing and innovative services.

If, however, the Commission decides that certain broadband and VoIP services are subject to CALEA, it should take great care in determining what CALEA compliance means for those services and not simply apply rules and methodologies designed for circuit-switched networks to these very different services. The Commission also should seek industry input before establishing guidelines to avoid establishing rules that are technically infeasible and unenforceable. And while “trusted third parties” may appear to be a viable compliance solution for many providers, the Commission should not mandate that providers use a trusted third party or simply rely on the existence of trusted third parties to determine whether compliance with CALEA is reasonably achievable.

Additionally, the Commission must not depart from the other statutorily-mandated processes and procedures in CALEA, such as the standards setting process, the extension process, and the enforcement procedures. All of these processes and procedures were enacted by Congress to ensure that CALEA was implemented in the way it envisioned. If Law Enforcement truly believes that a change in any of those processes or procedures is necessary, it should seek such a change from Congress.

And finally, the Commission must not hinder providers’ ability to seek cost recovery from Law Enforcement. Current surveillance laws clearly require Law Enforcement to pay for the assistance and facilities used in performing surveillance activities. While CALEA and Section 229 of the Communications Act arguably allow for additional means of cost recovery, neither supplants providers’ ability to seek and receive compensation directly from Law Enforcement.

II. BACKGROUND

A. SBC Fully Recognizes and Supports Law Enforcement's Legitimate Need to Conduct Lawful Surveillance Activities

Congress long ago recognized the vital need for Law Enforcement to conduct surveillance activities to prevent criminal conduct and safeguard the American people. As discussed below, Congress has provided Law Enforcement with a variety of statutory tools to perform these surveillance activities with regard to wire, oral or electronic communications. SBC has a long history of working cooperatively with Law Enforcement to ensure that Law Enforcement has the ability to obtain lawful surveillance of such communications. While new communications services, like the broadband and VoIP services at issue in the *CALEA NPRM*, raise new surveillance challenges, SBC is fully committed to continuing to work cooperatively with Law Enforcement to address these challenges and to ensure that Law Enforcement's surveillance needs continue to be met within the bounds of the law. Indeed, SBC believes that the only way to successfully address the surveillance issues associated with broadband and VoIP services is for all stakeholders, including the communications industry, Law Enforcement, and the Commission, to engage in a cooperative dialog aimed not just at identifying problems, but at finding solutions. It is within this spirit of cooperation that SBC files its comments in this proceeding

B. To Create an Appropriate Regulatory Framework under CALEA to Meet Law Enforcement's Surveillance Needs, the Commission Must First Understand the Statutory Source of Law Enforcement's Surveillance Authority

In the Omnibus Crime Control and Safe Streets Act (OCCSSA), Congress gave Law Enforcement the ability to conduct surveillance of wire or oral communications.[3] Under the procedures promulgated by Congress, Law Enforcement may apply to an appropriate federal or state judge for approval to conduct the surveillance, and the judge may grant the application if

[3] 18 U.S.C. §2516.

Law Enforcement is able to make the necessary evidentiary showings.[4] In addition, Congress gave Law Enforcement the ability to include in their applications a request for assistance from providers of communications services in conducting the surveillance, and obligated those providers to provide such assistance if a judge granted the application.[5] In 1986, Congress amended OCCSSA to allow Law Enforcement to obtain surveillance of "electronic communications," a broad category of communications that includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system . . . ."[6] Thus, OCCSSA (and other similar state statutes) establishes a framework by which Law Enforcement may obtain surveillance and imposes a general duty on providers of communications services to assist Law Enforcement in effectuating that surveillance.

CALEA, on the other hand, requires telecommunications carriers to build certain capabilities into their networks in order to enable those carriers to provide surveillance assistance to Law Enforcement. Unlike OCCSSA, CALEA does not grant Law Enforcement any ability to conduct searches, access networks, demand information, or perform surveillance; rather it requires that carriers build capabilities in their networks to more efficiently assist Law Enforcement in conducting lawful surveillance activities. Thus, even if Congress had never enacted CALEA, communications service providers would still have an obligation to assist Law Enforcement in effectuating lawful surveillance under OCCSSA. Accordingly, as the Commission moves forward in this proceeding, it should not rush to impose CALEA assistance obligations without sufficient industry input or set unreasonable CALEA implementation deadlines based on the erroneous perception that Law Enforcement lacks surveillance *authority* today.

---

[4] 18 U.S.C. §§2516 and 2518.

[5] *Id.*

[6] 18 U.S.C. §2510.

C. In Crafting Any Regulations to Implement CALEA, the Commission Should Be Mindful of How Law Enforcement Is Exercising its Surveillance Authority

To ensure that any final CALEA rules satisfy Law Enforcement's legitimate surveillance needs without unduly burdening service providers or impeding innovation, the Commission should be certain it understands the extent and manner in which Law Enforcement uses its surveillance authority so that it can craft appropriate rules. Publicly available data show that, on a national basis, Law Enforcement's surveillance activities are heavily concentrated in certain geographic locations and for certain technologies. According to the *2003 Wiretap Report*, published by the Administrative Office of the U.S. Courts, a total of 1,442 wiretaps were authorized by federal and state courts in 2003, which represents a 6 percent increase from 2002.[7] Of the 894 wiretaps authorized by state courts, 90 percent were authorized in just 7 states while 23 states authorized no wiretaps.[8] Seventy-seven percent of wiretaps in 2003 were authorized for mobile devices (e.g., cell phones), while less than one percent of wiretaps (or twelve wiretaps) were authorized for computers.[9]

While SBC in no way doubts the critical *importance* of the surveillance activities described in the *2003 Wiretap Report*, we urge the Commission to take into account the relatively limited *scope* of Law Enforcement's surveillance activities when considering how to implement CALEA. Even assuming an aggressive growth rate in Law Enforcement's need for surveillance in coming years, the number of annual wiretaps that communications service providers will need to facilitate for Law Enforcement is still quite small compared to the number of subscribers of modern communications services. In this regard, data from the Commission

---

[7] News Release - Administrative Office of the U.S. Courts, *Wiretap Authorizations Increase 2003* (Apr. 30, 2004) at 7.

[8] Those states are New York, California, New Jersey, Pennsylvania, Florida, Maryland, and Illinois. *Wiretap Report 2003* at 7.

[9] *Id.* at 10.

and other sources show that the U.S. has: over 181.4 million landline telephone lines;[10] approximately 160 million wireless telephone subscribers; [11] and over 28 million high speed (broadband Internet service) lines.[12] In establishing CALEA requirements, the Commission should give due consideration to the relatively limited need for wiretaps, at least until now, and should be careful not to impose costs on the industry and consumers that are disproportional to the benefits of the additional capabilities it mandates.

III. DISCUSSION

A. Any Commission Determination that CALEA Applies to Broadband and/or VoIP Services Must Be Based on a Solid Legal Rationale that Can Survive Judicial Review

Applicability of CALEA to Broadband and VoIP Services. In the *CALEA NPRM*, the Commission tentatively concludes that CALEA applies to certain types of broadband and VoIP services.[13] It bases this tentative conclusion on the so-called substantial replacement test prescribed by section 102(8)(B)(ii) of CALEA, which provides that a service provider may be deemed a telecommunications carrier subject to CALEA if that provider is "a person or entity engaged in providing wire or electronic communication switching or transmission service" and if "the Commission finds that such *service is a replacement for a substantial portion of the local telephone exchange service* and it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this title."[14] Specifically, the Commission tentatively concludes that broadband Internet access service and certain "managed" VoIP services satisfy

[10] FCC Statistics of Communications Common Carriers, Table 5.1 (2003/2004).

[11] *Id*. at Table 5.6.

[12] *Id.* at Table 5.4.

[13] NPRM at ¶¶47 & 56.

[14] 47 U.S.C. §1001(8)(B)(ii) (emphasis added).

the substantial replacement test and are thus subject to CALEA.[15] The Commission further opines that the provisions in CALEA excluding information services from the ambit of CALEA do not bar the application of CALEA to broadband Internet access service and managed VoIP services as described by the Commission (despite how those services may be classified under the Communications Act) because a contrary result would conflict with Congress's intent in enacting CALEA.[16]

Without generally expressing an opinion on the legal merits of the Commission's tentative conclusions about the applicability of CALEA to certain broadband and VoIP services,[17] SBC strongly urges the Commission to ensure that those conclusions are legally sustainable. Imposing CALEA obligations on the communications industry without a firm basis to survive judicial review will serve nobody's best interests. Service providers will have wasted valuable time, money and resources; Law Enforcement will lack certainty as to whether and how CALEA applies to new communications services; and the Commission will be forced to start again from the beginning. Thus, SBC encourages the Commission to make certain that its legal analysis is sufficiently rigorous to survive the judicial review that inevitably follows major Commission rulemaking proceedings.[18]

Competitive Neutrality. To the extent the Commission decides that any broadband and VoIP services are subject to CALEA, the Commission must ensure that the application of CALEA is competitively neutral. All service providers, regardless of the platform they use to deliver services (i.e. cable, DSL, wireless, satellite, powerline), should be subject to the same CALEA obligations. Of course, the manner in which those obligations are *implemented* may

[15] NPRM at ¶¶47 & 56, respectively.

[16] *Id*. at ¶50.

[17] *See* section II.B. of these Comments discussing the managed / non-managed distinction.

[18] To the extent the Commission does not believe CALEA, as written, allows it to expand the applicability in such a way so as to achieve the results desired by Law Enforcement, but believes those results are warranted, the Commission and/or Law Enforcement should seek modification of CALEA from Congress.

differ based on the technology used by a given provider, and the Commission should steer clear of mandating a "one-size-fits-all" approach, leaving open the ability for standards bodies to develop requirements based on the capabilities of each technology. But the general *obligation* to comply must apply evenly across the industry.

Future Services. Law Enforcement requested that the Commission establish rules stating that three types of future services and/or entities would be presumptively covered by CALEA.[19] Those requested rules would cover: (1) services that directly compete against a service already covered by CALEA, (2) entities that provide wiring or electronic communication switching or transmission service to the public for a fee, and (3) services utilizing a new technology that replace current packet-mode services covered by CALEA.[20] The Commission, however, relying upon the CALEA statute itself and Congressional intent, determined that such a rule would be "inconsistent with the statutory intent and could create an obstacle to innovation."[21] SBC agrees and urges the Commission not to embark on this highly-speculative and potentially unlawful endeavor. CALEA allows for expansion to cover new services as those services are developed in the marketplace, and specifically requires service providers and equipment manufacturers to work cooperatively to ensure that CALEA capabilities are available for services to which CALEA applies.[22] Adopting Law Enforcement's proposal and overriding the cooperative process that Congress spelled-out in CALEA in favor of Commission rules specifying the types of services to which CALEA applies would almost certainly run afoul of CALEA's prohibition against Law Enforcement dictating the design and development of

---

[19] *See* Joint Petition for Expedited Rulemaking Concerning the Communications Assistance for Law Enforcement Act RM-10865, filed March 10, 2004 (*LE Petition*) at 33-34.

[20] *Id.*

[21] NPRM at ¶61.

[22] CALEA Section 106; 47 U.S.C. §1005.

communications services and equipment.[23] The Commission would be wise to reject Law Enforcement's request

B. The Commission's Attempt to Distinguish between Managed and Non-Managed VoIP Services is Legally Suspect and Practically Unworkable

In the *CALEA NPRM*, the Commission tentatively concludes that "managed" VoIP services are subject to CALEA while "non-managed" VoIP services are not.[24] The Commission, using Law Enforcement's proposal, defines "managed" VoIP services as "those services that offer voice communications calling capability whereby the VoIP provider acts as a mediator to manage the communication between its end points and to provide call set up, connection, termination, and party identification features, often generating or modifying dialing, signaling, switching, addressing or routing functions for the user."[25] The Commission then describes "non-managed" VoIP services as those services "involv[ing] disintermediated communications that are set up and managed by the end user via its customer premises equipment or personal computer."[26]

While SBC generally does not offer an opinion on the merits of the Commission's preliminary determination to apply CALEA to VoIP services, SBC is concerned about the distinction the Commission attempts to draw between "managed" and "non-managed" services. As discussed above, under the substantial replacement test of section 102(8)(B)(ii), communications services may be subject to CALEA if those services become substantial replacements for local exchange service. Rather than focusing closely on whether a given VoIP service should be considered a substantial replacement for local exchange service, the Commission appears to have employed a proxy for that analysis – whether the service is

[23] CALEA Section 103(b)(1), 47 U.S.C. §1002(b)(1).

[24] NPRM at ¶¶56 & 58.

[25] *Id.* at ¶37.

[26] *Id.*

managed or not. But whether a service is "managed" by a service provider or not has little bearing on whether the service should be considered a substantial replacement for local exchange service. Indeed, rather than attempting to discern how service is managed by the *service provider*, the Commission should be focused on whether *end users* are using the service as a substantial replacement for local exchange service.

Moreover, while the Commission's attempt to draw a bright line for the applicability of CALEA is laudable in principle, the managed / non-managed distinction it proposes to that end is hopelessly unworkable in practice. Trying to devise a single list of functions that qualifies a service as "managed" would be a waste of time and resources and would provide little certainty to Law Enforcement or the industry. The level of communication management functions performed by service providers today varies widely across the industry. These management functions are not static; they are likely to change from provider to provider and service to service. As VoIP evolves, depending upon advances and technology and the needs of consumers, "non-managed" services may begin to look a lot like "managed" services and most likely will eventually include some of the capabilities that "managed" services do today. For instance, a peer-to-peer IP network could be highly managed, but still not be a substantial replacement for local exchange service because it is typically a "closed" network that does not allow communications with users on the PSTN. On the other hand, unmanaged peer-to-peer services could, in theory, supplant the PSTN over time, thus rendering them substantial replacements for the PSTN. As these examples indicate, the Commission's managed / non-managed dichotomy is not an accurate proxy for determining whether a service should be considered a substantial replacement for local exchange service and the Commission should abandon this line of analysis and instead rely on the substantial replacement test set forth by Congress in section 102(8)(B)(ii).

C. Assistance Capability Requirements Established for Legacy Services Must be Updated and Clarified Before They Can Be Applied to Broadband and VoIP Services.

Section 103 of CALEA sets forth the obligations that telecommunications carriers have in designing their networks and services to assist Law Enforcement in conducting surveillance. As the Commission points out in the *CALEA NPRM*, section 103 requires telecommunication carriers to "enable [Law Enforcement], pursuant to a court order or other lawful authorization, (1) to intercept, to the exclusion of other communications, wire and electronic communications carried by the carrier to or from a subject, and (2) to access call-identifying information that is reasonably available to the carrier, subject to certain conditions."[27] While the Commission has more fully articulated the scope of these two obligations for legacy, circuit-switched services,[28] and the industry has developed the means to implement these obligations for such legacy circuit-switched services, the Commission and the industry have not had the opportunity to fully explore how these obligations should apply to broadband Internet access services and VoIP services. Indeed, these services are quite different from POTS, and they should not and cannot be treated the same as POTS for CALEA purposes. As discussed below, there are major differences in network configuration, equipment, and other aspects of these services that need to be fully explored by the industry and the Commission before the capability requirements of section 103 can be effectively implemented.

[27] *Id.* at ¶63.

[28] *Id.* at ¶¶63-64. *See also Communications Assistance for Law Enforcement Act*, Order on Remand, 17 FCC Rcd 6896 (2002) ("*CALEA Order on Remand*"), at 6911, ¶¶34 & 48.

1. Interception Cannot be Performed on Broadband and VoIP Services in the Same Manner as It Is on Local Telephone Exchange Service.

In many instances, regardless of the network infrastructure, broadband providers simply will not have access to the same level of call content, nor be able to perform the same type of interception, as telecommunications providers can with the PSTN. The primary reason for this distinction is that these services are packetized, not circuit-switched. Unlike circuit-switched services on the PSTN, the packets transmitted in a typical broadband Internet access service do not run in single direction, or all together in a single stream, allowing for easy interception. Furthermore, broadband providers will rarely be able to identify which packets are performing what tasks. In other words, a broadband provider typically cannot distinguish between a voice packet, data packet, or video packet without additional information from the user or content provider or without adding certain equipment to its network, which would not be essential to the network for any purpose other than CALEA compliance. Thus, broadband providers are typically unable to "see" the application level information contained in each packet. This renders identifying the right packets for interception difficult, if not impossible, and protecting users privacy an almost unattainable task.

In addition, unlike traditional local telephone service, broadband Internet access service is not always provided to the end user by a single provider. A broadband customer may utilize broadband transport from one provider (e.g., DSL service from a LEC) while obtaining Internet access from a separate provider (e.g., an independent ISP). In such circumstances, it is not possible for the broadband transmission provider to perform all of the functions specified in section 103 of CALEA (including the requirements to safeguard the privacy of certain information from Law Enforcement or collect call-identifying information) because that provider does not control the entire service and can only provide access to the information that traverses its network.

VoIP presents its own unique set of interception challenges. While trial-use CALEA standards have recently been established , there are portions of those standards that may not be achievable for all VoIP services due to the differences in software and hardware utilized by different VoIP providers. Additionally, those standards do not address the type of interface necessary to retrieve call content and call identifying information and lack sufficient technical specifications to enable equipment manufacturers to build the capabilities into their products that will allow for vendor interoperability. Moreover, in order to intercept a VoIP call, extensive coordination between various entities may be required, many of which ordinarily do not have any direct relationship with each other. In today's VoIP world, an end-user could have one provider for its VoIP service and a different provider for Internet access (which, as discussed above, may be provided by two separate entities). In addition, the VoIP provider, who has the relationship with the end user, could be "outsourcing" portions of its VoIP service to separate wholesale VoIP providers. Providing surveillance capabilities for a single call may require extensive coordination among these different providers.

While such coordination may not be impossible, much work must be done within the industry to establish whether and how such coordination should be accomplished. But as noted by Congress, CALEA, "is not intended to guarantee 'one-stop shopping' for law enforcement."[29] Thus, before the Commission adopts any CALEA regulations in this proceeding, it must first work with the industry to provide clear guidance about the obligations that apply to broadband Internet access and VoIP services under section 103.[30]

2. The Commission, With Industry Input, Needs to Define "Call-Identifying Information" for Broadband and VoIP Services

In addition to having the capability to intercept the content of a communication, section 103 of CALEA also requires telecommunications carriers to provide "call-identifying information." CALEA defines call-identifying information as "dialing or signaling information

[29] House Report at 3502.

[30] In section III.D. of these Comments, SBC offers proposals for producing such guidance.

that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier."[31] The Commission adopted the following definitions of each of those components of call-identifying information:

> **origin** is a party initiating a call (*e.g.*, a calling party), or a place from which a call is initiated; **destination** is a party or place to which a call is being made (*e.g.*, the called party); **direction** is a party or place to which a call is re-directed or the party or place from which it came, either incoming or outgoing (*e.g.*, a redirected-to party or redirected-from party); and **termination** is a party or place at the end of the communication path (*e.g.*, the called or call-receiving party or the switch of a party that has placed another on hold).[32]

While these definitions may have made sense in a circuit-switched environment, they do not readily correspond to the way packet-switched services like broadband Internet access and VoIP are provided Indeed, the Commission has recognized that the traditional geographic concepts of origination and termination may not be applicable in an IP environment because IP-based services are routed to IP devices not particular geographic locations.[33] Thus, the Commission will need to reevaluate how call-identifying information should be defined for broadband and VoIP services. In fact, the Commission appears to recognize this fact when it suggests that, in the context of broadband Internet access service, call-identifying information may include, "(1) information about the subject's access sessions, (2) information about changes to the subject's service or account profile…and (3) information about packets sent and received by the subject, including source and destination IP addresses, information related to the detection and control of packet transfer security such as those in Virtual Private Networks

---

[31] CALEA Section 102(2), 47 U.S.C. §1001(2).

[32] NPRM at ¶64. *See also* *CALEA Order on Remand* at 6907-08, ¶34 and 47 C.F.R. §§22.1102, 24.902, 64.2202.

[33] Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service, WC Docket No. 03-45, *Memorandum Opinion and Order*, 19 FCC Rcd 3307 (2004).

("VPNs"), as well as packet filtering."[34] But as discussed above, a broadband or VoIP end user may be obtaining its service from a combination of different providers and some of the call-identifying information listed by the Commission may be accessible only to a subset of those providers, or even a single provider. Thus, before determining how to define call identifying information for broadband Internet access and VoIP services, the Commission should ensure that it works through these difficult issues together with industry experts in the manner proposed by SBC in the following section.

D. The Commission Should Obtain Detailed Technical Input from Industry Experts through Working Groups and Forums Before Establishing Specific Regulations Regarding CALEA Capabilities for Broadband and VoIP Services.

Although the Commission has sought general comment on how the capability requirements of section 103 of CALEA should be applied to broadband Internet access and VoIP services, there are a plethora of complex issues concerning the proper application of section 103 to these services (discussed above) that are not going to be resolvable based on the record developed in response to the *CALEA NPRM*. The industry needs an opportunity to work in a collaborative fashion to examine these issues and achieve at least a modicum of consensus as to how section 103 can be applied to broadband and VoIP services – especially in light of the multiple providers involved in providing a single service to an end user.

It is also important to ensure that the industry and the Commission, not Law Enforcement alone, are driving the determinations about the nature of CALEA obligations under section 103 for broadband and VoIP services. Congress specifically prohibited Law Enforcement from requiring a specific design or configuration for CALEA compliance and from banning the adoption of equipment, facilities, services, or features.[35] Instituting specific rules in response to Law Enforcement's petition with regard to the services in question in this rulemaking without adequate industry examination and discourse would be in contravention of Congress' specific direction.

[34] *NPRM.* at ¶66.
[35] *See* Section 103(b)(1) of CALEA, 47 U.S.C. §1002(b)(1).

Thus, to ensure that any section 103 requirements are applied to broadband and VoIP services in a technically feasible manner consistent with Congress's intent, the Commission should take a leadership role in bringing industry together in a collaborative effort to address CALEA obligations for these services. While there are many permutations of industry fora, three specific ways in which the Commission could open this discourse would be (1) through an industry group similar to the one jointly led by ATIS and Law Enforcement in the early days of CALEA, the Electronic Communications Service Provider Committee (ECSP), (2) Joint Expert Meetings (JEMs), and/or (3) an inquiry and report from a Commission-appointed industry expert akin to the Hatfield inquiry and report on technical and operational issues affecting wireless E911 services.[36]

Any or all of these approaches would allow for a more thorough examination of the problems and issues specifically associated with each of these services and would aid the Commission in making its final determinations. Without obtaining expert input, the Commission would be establishing rules in a vacuum, with the only true input coming from Law Enforcement itself. SBC does not intend to imply that Law Enforcement should not play a role in these determinations, but it should not be the sole arbiter. Law Enforcement does not have the technical expertise or operational insight to either know how the various providers' services will be impacted by the rules that may be established by this rulemaking or to understand that there may be even better, more efficient, less costly ways to implement CALEA that are acceptable to all parties involved. Accordingly, as discussed in more detail below, SBC strongly encourages the Commission to consider obtaining detailed input from industry experts through some or all of the approaches identified above.

First, although there was not a full consensus in the ECSP meetings, those meetings , which were co-chaired by the industry and the FBI, were highly successful in creating, not only a dialog between the various carriers, but also between the carriers and Law Enforcement. This dialog was the springboard for eventual industry consensus and initial CALEA standards, which

[36] *See* Report on Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Services, WT Docket No. 02-46 (2002).

have enabled carriers in the circuit switched world to provide Law Enforcement with the type of access capabilities envisioned by CALEA. The same type of forum could work with broadband and VoIP.

Second, JEM meetings were quite successful in producing a thorough, independent analysis of the FBI's Carnivore technology, which has enabled Law Enforcement to perform numerous intercepts of packetized communications. It is therefore reasonable to assume that a similar group could address the implications of applying CALEA regulations to broadband and VoIP services. Such an analysis could aid the Commission in making CALEA-related decisions with respect to these services.

Third, the Commission's experience in addressing the technical issues surrounding wireless E-911 implementation could also serve as a useful model for addressing CALEA. Specifically, the Commission appointed a leading industry expert and former Chief of the Office of Engineering and Technology, Dale Hatfield, to conduct an inquiry and prepare a report on the technical and operational challenges to implementing wireless E-911 capability. The subsequent Hatfield Report, and the recommendations contained therein, provided the Commission with valuable guidance to address these challenges and served as an important guidepost for subsequent Commission decision making on wireless E-911. The Commission could benefit immensely from a similar approach for CALEA. By appointing a respected industry expert, or panel of experts, and tasking them with conducting an inquiry and preparing a report on the technical and operational challenges in applying CALEA to broadband and VoIP services, the Commission would gain the type of information necessary to craft appropriate CALEA rules for these services.

With all of these proposals, the Commission could establish reasonable timeframes for the production of any recommendations or reports (e.g., 12 months) to ensure that the establishment of assistance obligations for broadband and VoIP services under section 103 proceeds in a timely manner to meet the needs of Law Enforcement. Indeed, Law Enforcement's surveillance needs, at least in the short term, appear primarily focused on wireless telephony services.[37] While SBC does not dispute Law Enforcement's longer term needs for surveillance of broadband and VoIP services, it is far more important at this juncture for the Commission to specify *appropriate* CALEA obligations rather than simply hurrying to announce CALEA obligations for services that are only minimally surveilled today.[38]

E. The Trusted Third Party Solution Should Be An Option, Not A Requirement.

In the NPRM, the Commission seeks comment on the possibility of allowing telecommunications carriers to use a trusted third party (TTP) to "manage the intercept process."[39] Essentially, a telecommunications carrier would "outsource" its compliance obligations under section 103 to the TTP and the TTP would provide Law Enforcement with the appropriate intercept or call-identifying information. Under the TTP approach, the telecommunications carrier would still retain the ultimate legal responsibility for CALEA compliance, but would be able to use the TTP to meet that responsibility.

SBC believes the Commission should allow, but not require, telecommunications carriers to use TTPs to meet their CALEA compliance obligations. TTPs could prove to be a more cost effective solution than having each carrier subject to CALEA take on all compliance responsibilities itself. The *potential* cost savings are particularly attractive given that many carriers apparently do not receive any surveillance requests during the course of a typical year. If those savings materialize, carriers will have incentive enough to use TTPs without a regulatory mandate.

While SBC thus believes carriers should have the option of using a TTP to provide surveillance information to Law Enforcement, the Commission should bear in mind that Law

---

[37] *See* Section II.C. above.

[38] Of course, as discussed above, even in the absence of any specific CALEA obligations, service providers already have an *existing* duty under OCCSSA to assist Law Enforcement in conducting surveillance on broadband and VoIP services.

[39] NPRM at ¶69.

Enforcement must by law compensate carriers for certain surveillance costs, irrespective of whether those carriers choose to use a TTP.[40] In particular, section 2518 of OCCSSA requires Law Enforcement to bear, the costs for circuits, traffic aggregation, mediation devices, and backhaul. That will continue to be the case regardless of whether a TTP is used as a mediator in gathering and deciphering the information given to it by carriers.

Given that it is Law Enforcement that will be using the information and has the statutory responsibility for paying for it, it might be most efficient for Law Enforcement to utilize TTPs as their agents in gathering and deciphering the appropriate information. Under this approach, telecommunications carriers would still have an obligation under section 103 to maintain appropriate interfaces in their networks to allow TTPs to obtain that information, but Law Enforcement, through its direct relationship with the TTP, would be in a better position to ensure that it obtains the information it needs in the format that it desires. For example, in the case of broadband, carriers could provide the full data stream to TTPs and the TTPs would then extract the information needed by Law Enforcement and provide it to Law Enforcement in the manner most suitable to Law Enforcement.

If the Commission nonetheless were to decide that telecommunications carriers, rather than Law Enforcement, should have the responsibility of establishing TTP relationships, the Commission must recognize that TTPs may not be the best answer for all carriers in all instances. The Commission assumes that because a single TTP could service many carriers, such a paradigm would result in cost savings for those carriers.[41] But in fact, given the limited number of TTP vendors and depending upon the configuration of the TTP solution, the cost of TTP service may be prohibitive in some circumstances. Thus, just because a TTP solution exists, the Commission should not automatically determine that CALEA capabilities are

[40] SBC addresses general cost recovery issues for CALEA in section III.H. of these Comments.

[41] NPRM at ¶72.

reasonably available in all circumstances.[42] Accordingly, while the Commission should explore the TTP approach as an option, it should not impose the TTP approach as a mandatory requirement.

F. The Commission Should Not Depart from the Standard Setting Process Established By Congress

In section 107 of CALEA, Congress spelled out a process by which telecommunications carriers can comply with the assistance obligations in section 103 by implementing industry-developed, safe harbor standards. Under CALEA section 107(a), Law Enforcement has an obligation to consult with industry standards-setting bodies to develop these safe harbor standards. If a telecommunications carrier implements these standards, it will be deemed in compliance with its obligations under CALEA section 103. In the event that standards are not developed, or if a party believes that any standards are deficient, section 107(b) establishes a procedure for the Commission to establish the requisite standards. Thus, by creating section 107, Congress wisely expressed a strong desire for industry experts in standards bodies, not Law Enforcement, to take the lead in establishing the technical standards for CALEA.

1. The Commission Should Not Assess the Sufficiency of Packet-Mode Standards in this Proceeding, But Should Require Law Enforcement to File a Deficiency Petition if it Believes Those Standards to be Deficient

As the Commission points out in the NPRM,[43] Law Enforcement has been extremely critical of some of the standards setting processes and goes so far as to state that the "packet mode standards that have been published are deficient."[44] The Commission then seeks comment

[42] The Commission tentatively concluded that the mere availability of a TTP approach would render call-identifying information "reasonably available" to providers under Section 103(a)(2). NPRM at ¶70. While the availability of a TTP solution may be enough to pass the test of reasonable availability under that Section, if the cost are high, it should fail the test of reasonable availability under Section 109(b).

[43] NPRM at ¶78

[44] *LE Petition* at 35.

on the packet-mode standards and states that it seeks such comment "in an attempt to determine whether any of these standards are deficient."[45] The petition for rulemaking filed by Law Enforcement, however, is not the proper vehicle for the Commission to use in deciding whether any particular standard is deficient. If Law Enforcement believes that certain standards are deficient, it must specifically petition the Commission to establish appropriate technical requirements or standards in accordance with the procedures set forth in section 107(b). Law Enforcement has not filed such a petition and, therefore, the Commission should not make any determinations regarding the deficiency of the packet-mode standards in this rulemaking.

G. Compliance Issues: Extensions, Timelines and Enforcement

1. The Commission Should Not Alter The Extension Petition Process

Section 107(c) of CALEA allows carriers to file a petition for extension if they are unable to comply with the section 103 capability requirements within the compliance period. The Commission proposes, in the NPRM, to "restrict the availability of compliance extensions under section 107(c), particularly in connection with packet-mode requirements."[46] This proposal is in direct contravention of Congressional intent. Section 107(c)(1) specifically gives carriers the right to seek an extension if they cannot comply with section 103 within the prescribed period. And section 107(c)(2) gives the Commission the authority to grant extensions, as well as the basic grounds – "compliance with the assistance capability requirements under section 103 is not reasonably achievable through an application of technology available within the compliance period" – under which to grant those extensions. The Commission cannot predetermine that such flexibility, as allowed under statute, should be restricted. While Congress clearly did not intend for the Commission to issue extensions that would go on forever, Congress recognized

[45] NPRM at ¶81.

[46] *Id*. at ¶87.

that, in at least some cases, compliance with requirements would not be reasonably achievable within the four-year compliance period established by CALEA.[47]

Congress understood that compliance with CALEA could require new technological development and major changes in telecommunications networks. Congress accordingly made sure to provide adequate time both for the development of workable industry standards and for implementation of those standards. Congress was open to giving carriers up to six years to implement CALEA (the initial four years to comply plus an additional two years if an extension was necessary). The need for adequate time is even more compelling with respect to broadband and VoIP which pose unique CALEA challenges. As stated throughout these comments, packet-based services are completely different from circuit-switched services. They would require substantial, potentially costly, changes in order to meet section 103 requirements. If the Commission makes the determination that broadband and VoIP services are subject to CALEA regulation, it is all the more important that the Commission give the providers of these services the time Congress intended them to have to implement CALEA.

For these reasons, SBC does not support a change to the extension petition process or a tightening of the extension requirements. This process is necessary given all of the parties (carriers, vendors, etc.) that must work together to implement new standards and changes to networks. And broadband and VoIP service providers should be afforded the same opportunity for extension that other providers were afforded in order to work with the industry and Law Enforcement to develop standards that will ensure compliance with CALEA without jeopardizing networks or the evolution of new technology.

---

[47] Section 111(b) (which appears as 47 U.S.C. §1001 note), provided that the requirements under Sections 103 and 105 would take effect 4 years after the enactment of CALEA. *See also* House Report at 3508, which discusses section 107(C) extensions.

2. The Commission's Recommended Implementation Timeline Is Unreasonable

In its NPRM, the Commission states that it supports Law Enforcement's goal of strengthening CALEA implementation, but it believes that goal "can be achieved without us imposing the implementation deadlines and benchmark filings it requests."[48] SBC agrees that if the Commission determines that CALEA applies to broadband and VoIP services, a reasonable implementation plan is necessary to spur cooperation in the industry and between the industry and Law Enforcement. But SBC agrees that the Commission should not, and arguably cannot, establish the draconian benchmarking process recommended by Law Enforcement.

In proposing a specific implementation timeline, the Commission first appears to be on track with its earlier pronouncements, stating that it intends, "to afford all carriers a reasonable period of time in which to comply with, or seek relief from, any determinations that we eventually adopt."[49] It then goes on, however, to recommend 90 days as the "reasonable period" for complying with or seeking relief from the requirements the Commission adopts. SBC believes that 90 days is flatly unreasonable – all the more so, given the Commissions suggestion that extensions of the ninety-day period will be extremely difficult for carriers to obtain.[50]

SBC believes it will take far longer than 90 days to fully implement CALEA solutions for packet-mode services and more than the 15 months recommended by Law Enforcement and endorsed by the Commission for the other services at issue in this rulemaking. The exact amount of time, of course, cannot be determined until the Commission establishes the ultimate requirements, including the definitions for call-identifying information. Therefore, the Commission should quickly establish the industry forum or workshops to begin the necessary industry discussion regarding capabilities, limitations, and responsibilities. Then, the Commission must allow a reasonable amount of time for the industry to establish parameters for

---

[48] NPRM at ¶91.

[49] *Id.*

[50] *Id.* at ¶¶97 & 99.

the standards bodies to later use in developing standards. In order to truly produce meaningful results that process should be given at least 12-18 months. It would then be up to the open, public standards bodies to develop the requisite standards for these services. And in the meantime, Law Enforcement has the capability to continue lawful intercepts and data gathering by means available today.

If, however the Commission declines the opportunity to get input from the industry and, instead, chooses to establish the parameters suggested in this rulemaking, it could take much longer for carriers to implement the appropriate technology to achieve those goals. Without proper guidance and a clear understanding of their responsibilities, many carriers may never be able to implement the solutions suggested in this NPRM. Thus, it would better serve the interests of Law Enforcement and industry alike, if the Commission follows the course of action outlined above and declines to adopt arbitrary deadlines for CALEA compliance.

3. New CALEA Enforcement Procedures Are Not Necessary And Are Not Within The Commission's Authority Under CALEA

Law Enforcement has requested that the Commission establish specific rules to enforce CALEA compliance because Law Enforcement is concerned that lack of Commission enforcement has contributed to problems and delays in CALEA implementation.[51] In the NPRM, however, the Commission recognizes that Congress assigned the role of CALEA enforcement to the federal courts. Indeed, Congress specifically established enforcement mechanisms for CALEA in section 108.[52] That section gives a court the ability to require carriers to implement CALEA, and section 2522 of OCCSSA empowers a court to fine carriers

[51] *LE Petition* at 58.

[52] Section 108 allows for a court order enforcing CALEA compliance. It limits the grounds for issuance ***only*** to findings that "(1) alternative technologies or capabilities or the facilities of another carrier are not reasonably available to law enforcement for implementing the interception of communications or access to call-identifying information; and (2) compliance with the requirements of this title is reasonably achievable through the application of available technology to the equipment, facility, or service at issue or would have been reasonably achievable if timely action had been taken." 47 U.S.C. §1007(a)(1-2).

up to $10,000 per day for failing to comply with CALEA. Thus, Congress has already provided ample enforcement authority to ensure that CALEA compliance and theRe is no need for the Commission to create additional enforcement mechanisms of its own.

Moreover, as the Commission further points out, many commenters to Law Enforcement's petition argued that a separate enforcement scheme may violate Congress's desire to create an exclusive enforcement scheme for CALEA in section 108,[53] and thus the Commission may not have authority to adopt such an enforcement scheme even if it wanted to do so. SBC agrees with these commenters and urges the Commission not to adopt a redundant and potentially unlawful enforcement mechanism for CALEA.

H. The Commission Should Establish A Reasonable Cost Recovery Mechanism for CALEA That Ensures All Providers Are Afforded the Opportunity To Recover Their Costs

In its petition, Law Enforcement urged the Commission to establish rules that would effectively place all of the costs of CALEA compliance for broadband and VoIP service onto service providers and their customers. Specifically, it has asked the Commission to do three things:

> (1) confirm that carriers bear the sole financial responsibility for development and implementation of CALEA solutions for post-January 1, 1995 communications equipment, facilities, and services, (2) permit carriers to recover from their customers the costs of developing and implementing CALEA intercept solutions in post-January 1, 1995 equipment, facilities, and services; and (3) clarify the methodology for determining carrier CALEA intercept provisioning costs and who bears financial responsibility for such costs.54

Law Enforcement focuses this discussion of cost recovery solely on CALEA. The discussion of cost recovery, however, should begin with the first statute dealing with carriers' obligations to assist Law Enforcement in its surveillance activities – OCCSSA – before delving into any

[53] NPRM at ¶113.

[54] *LE Petition* at 63.

additional permitted means of cost recovery established under CALEA or section 229 of the Communications Act.

1. Providers Are Entitled to Recover, From Law Enforcement, Costs Incurred in Providing Facilities or Assistance to Law Enforcement

Section 2518(4) of OCCSSA specifically states, "[a]ny provider of wire or electronic communication service, landlord, or custodian or other person furnishing such facilities or technical assistance [to law enforcement] *shall* be compensated therefore by the applicant [law enforcement] for reasonable expenses incurred in providing such facilities or assistance."[55] This not only specifically permits carriers to recover, from Law Enforcement, the costs of providing facilities to Law Enforcement for the purposes of performing surveillance activities, but explicitly directs Law Enforcement to compensate carriers for the costs of those facilities.

The Commission mentions in the *CALEA NPRM*, "as a general rule, LEAs must compensate carriers for their costs associated with provisioning a court-authorized intercept."[56] And the NPRM further makes note of Law Enforcement's acknowledgment that "Title III of the OCCSSA generally authorizes carriers to recover intercept provisioning costs from law enforcement."[57] The fact that both the Commission and Law Enforcement seem to agree that Congress intended for providers to charge Law Enforcement for the costs incurred in providing facilities for intercepts should demonstrate that there is no doubt about this fundamental point.

Despite these acknowledgments, the Commission and Law Enforcement focus primarily on the cost recovery mechanisms established under CALEA to claim that carriers are responsible for post-January 1, 1995, CALEA-related costs. The Commission and Law Enforcement misread the applicable cost recovery mechanisms.

OCCSSA provides basic framework for the recovery of surveillance costs. Indeed, the Commission has previously recognized as much. In its *CALEA Order on Remand*, the

---

[55] 18 U.S.C. § 2518 (emphasis added).

[56] NPRM at ¶132.

[57] *Id*. at ¶133. *See also LE Petition* at 68.

Commission confirmed that carriers could recover those costs from Law Enforcement by including capital costs in the per intercept fee carriers charge to Law Enforcement. The Commission specifically stated:

> carriers can recover at least a portion of their CALEA software and hardware costs by charging [agencies], for each surveillance authorized by CALEA, a fee that includes recovery of capital costs, as well as recovery of specific costs associated with each order.58

Neither the Commission or Law Enforcement has proffered a valid legal or factual basis to depart from that conclusion. Clearly, requiring Law Enforcement to pay for surveillance capabilities places the burden of the costs exactly where Congress intended – on Law Enforcement. Therefore, the Commission's tentative conclusion that "carriers bear the responsibility for CALEA development and implementation costs for post-January 1, 1995 equipment and facilities"[59] is clearly wrong. It is not within the Commission's authority to shift the burden to carriers and prohibit carriers from recovering their costs directly from Law Enforcement.

Indeed, section 109(b) of CALEA does not repeal the cost recovery provisions of OCCSA, and it certainly does not shift cost recovery to carriers; it simply shifts the compensation obligation from local, state, and federal law enforcement agencies to the Attorney General of the United States in circumstance where compliance with CALEA is not reasonably achievable. Section 109(b) of CALEA specifically states that first the Commission must determine, within one year of the filing of a petition by a carrier, whether compliance with

[58] *See CALEA Order on Remand* at 6917.

[59] NPRM at ¶125.

CALEA Section 103 requirements is reasonably achievable.[60] If the Commission determines that compliance is not reasonably achievable, then the Attorney General may agree to pay the carrier for the additional reasonable costs of compliance or, if the Attorney General does not agree to pay those costs, the carrier will be deemed to be in compliance.[61] Therefore, for those carriers that must perform extraordinary measures to become CALEA compliant, the Attorney General can determine whether those upgrades are so vital that they warrant extraordinary cost-recovery, i.e. direct payment from the Federal government.

CALEA, however, does not directly speak to the question of who bears the costs if compliance *is* reasonably achievable. It is reasonable to assume that Congress did not have to answer this question, given the long-standing cost recovery mechanism established under OCCSSA. Congress intended that carriers would continue to recover the costs of providing facilities for intercepts from Law Enforcement as they had been recovered for over 20 years. In fact, legislative history demonstrates that Congress enacted a cost recovery mechanism in CALEA not to override existing OCCSSA means of cost recovery, but to supplement it. Congress recognized that existing equipment, services, and features would have to be retrofitted to comply with the new CALEA requirements and since those network upgrades were going to be extensive and would occur over a relatively short period of time, it provided for the Federal government to cover the reasonable costs incurred in performing those upgrades.[62] This is also why Congress allowed for an additional means of cost recovery for post-January 1, 1995 equipment, facilities, and services if the Commission determines that compliance is not reasonably achievable. In those instances, extraordinary measures would have to be taken to achieve CALEA compliance, so Congress enacted extraordinary means of cost recovery – from

---

[60] CALEA Section 109(b)(1), 47 U.S.C. § 1008(b)(1).

[61] CALEA Section 109(b)(2), 47 U.S.C. § 1008(b)(2).

[62] *See* House Report at 3490.

the Attorney General rather than a specific Law Enforcement agency – to ensure that the carrier would be compensated and Law Enforcement agencies would not have to pay an exorbitant price for interceptions. Upgrades that are reasonably achievable are those that, presumably, could be performed at a lower cost, since cost is a factor in determining reasonable achievability.[63] In that case, the costs to implement those changes in equipment or facilities would be more easily recoverable through the ordinary OCCSSA cost recovery mechanism – directly from the requesting Law Enforcement agency.

In addition, Section 229(e) of the Communications Act addresses CALEA cost recovery mechanisms and establishes the Commission's role in CALEA cost recovery. This section essentially gives the Commission general oversight with respect to CALEA cost recovery and further authorizes it to permit common carriers (as defined under the Communications Act) to adjust their charges to recover CALEA-associated costs. It is thus reasonable to surmise that Congress enacted section 229(e) to enable the Commission to oversee carrier cost recovery for common carriers with respect to OCCSSA intercept costs, given that those charges may be adjusted to include CALEA costs.

2. The Commission Has the Authority to Permit Providers to Recover CALEA-Related Costs from Their Customers and Should Publicly Acknowledge That Providers Have A Legitimate Right to Do So

Law Enforcement requested that the Commission establish rules "permitting carriers to recover the cost of post-January 1, 1995 CALEA requirements from their customers."[64] The Commission seeks comment on whether it has the authority to permit such a charge.[65] SBC believes that the Commission need not address this issue since Law Enforcement must by law compensate carriers for their CALEA costs. If, however, the Commission concludes otherwise,

---

[63] CALEA at Section 109(b), 47 U.S.C. § 1008(b)

[64] *LE Petition* at 63.

[65] *NPRM* at ¶127.

section 229(e) of the Communications Act is broad enough to give the Commission the authority to impose or allow an end-user charge to recover CALEA-related costs.[66]

IV. CONCLUSION

For the foregoing reasons, the Commission should carefully examine whether broadband and VoIP services truly fit into the current CALEA statute and make such a determination only if the Commission is confident that it will withstand judicial scrutiny. If the Commission does choose to make such a determination, it should first establish and seek the counsel of an industry forum to ascertain the scope of applicability for each service. Once the scope has been determined, standards bodies should be allowed to perform as they have in the circuit-switched world and develop appropriate standards for the various "flavors" of both broadband Internet access and VoIP. Providers of both types of services should be allowed ample time to implement those standards and should be allowed a reasonable form of cost recovery for the necessary changes required by the new standards.

Respectfully Submitted,

/s/ Jennifer Brown

Jennifer Brown
Gary L. Phillips
Paul K. Mancini

SBC Communications Inc.
1401 I Street NW 11th Floor
Washington, D.C. 20005
Phone: 202-326-8904
Facsimile: 202-408-8745

Its Attorneys

November 8, 2004

[66] 47 U.S.C.§229(e).